Annual 47 CFR § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: **2/6/2019**

2. Name of company(s) covered by this certification: **Tower Net Communications, Inc.**

3. Form 499 Filer ID: **832057**

4. Name of signatory: **Drew Vermette**

5. Title of signatory: **Vice President**

6. Certification:

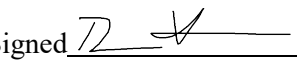
I, **Drew Vermette**, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Drew Vermette
VP, Tower Net Communications, Inc.

Attachments: Accompanying Statement explaining CPNI procedures

Accompanying Statement to
Annual CPNI Compliance Certification
CPNI Procedures

In compliance with 47 C.F.R. § 64.2001 et seq, I, Drew Vermette, officer of Tower Net Communications, Inc. (**"Tower Net"**), certifies that the company has taken the following steps in compliance with the rules of the Federal Communications Commission which govern the protection of Customer Proprietary Network Information (CPNI).

The following operating procedures ensure that Tower Net is in compliance with the FCC's CPNI Rules:

Tower Net does not make available to any affiliated or unaffiliated entity information which meets the definition of CPNI set forth at 47 U.S.C. § 222(h)(l), except when required to do so by law.

Tower Net only uses CPNI to render, and bill for, the telecommunications services it provides to its customers. Tower Net does not use its customers' CPNI for any marketing purpose, either internal or external, or other purpose set forth in the FCC's CPNI Rules, 47 C.F. R. § 64.2001 et seq.

Tower Net has practices and procedures that govern the disclosure of CPNI:

- Tower Net does not disclose or release CPNI upon a customer's telephone request.
- Tower Net does not disclose or release CPNI through online access over the Intemet.
- With respect to telephone inquires by customers concerning specific call related issues, Tower Net requires the customer to provide sufficient specific information about the call in question to confirm the customer's identity.
- Tower Net automatically notifies customers (at the customer's original telephone number or address on file) in case any changes are made to the customer's primary account information.
- Tower Net is prepared to notify the required U.S. government agencies in the event of a breach of the CPNI rules and to provide the required notice to affected customers of any such breach.

Tower Net provides training to all relevant employees on the company's practices and procedures that protect CPNI and its misuse.

It is a violation of Tower Net's polices to disclose CPNI outside of Tower Net. Any employee that is found to have violated this policy will be subject to disciplinary action up to and including termination.

Access to CPNI at Tower Net is restricted to a limited number of employees and controlled through the use of active security and other measures, including the use of special passwords that are assigned on a limited basis and technological measures which prohibit the electronic reproduction or distribution of CPNI. Encryption and other security practices are utilized when CPNI is transmitted electronically.

Strict controls are in place involving responses to law enforcement agencies that serve Tower Net with valid legal demands, such as a court ordered subpoena, for CPNI. Tower Net will not supply CPNI to any law enforcement agency that does not produce valid legal demand.